What is claimed is:

1. A method comprising:

identifying a firmware upgrade request by a firmware program;

retrieving a file signed with a private key;

validating the file with a public key;

upgrading a portion of the firmware program by the firmware program; and

locking a device storing the firmware program such that a second portion of the firmware program is not readable.

2. The method of claim 1, further comprising:

validating the public key; and

retrieving a second public key from the firmware program if the public key is not valid.

3. The method of claim 1, identifying a firmware upgrade request by a firmware program further comprising:

reading a flag, wherein the flag is located in a non-volatile medium; and

determining that the flag is set.

4. The method of claim 3, further comprising:

deleting the file; and

clearing the flag.

5. The method of claim 1, further comprising:

determining that the file is not authentic; and

locking the device.

6. The method of claim 1, further comprising:

locking the device after upgrading a portion of the firmware program by the firmware program.

7. The method of claim 1, wherein the second portion of the firmware program is a public key.

8. A method comprising:

identifying an upgrade request for a firmware program of a system;

upgrading a first public key of the firmware program;

receiving an interruption of power to the system; and

using a second public key to subsequently upgrade the firmware program.

9. The method of claim 8, further comprising:

retrieving a file signed by a private key from the system; and

authenticating the file with the second public key.

10. The method of claim 9, further comprising:

locking the device such that a portion of the firmware program is not readable.

11. The method of claim 10, locking the device such that a portion of the firmware program is not readable further comprising locking the device such that the public keys are not readable.

12. The method of claim 9, further comprising:

locking the device such that the public keys are not writable.

13. A system comprising:

a file signed by a private key;

a device for storing a program, wherein the device may lock access to the program; and

a firmware program stored in the device, which, upon execution:

determines that an upgrade flag is set;

retrieves the file;

validates the file using a public key;

upgrades a portion of the firmware program; and

locks the device such that the a portion of the firmware program is not readable.

14. The system of claim 13, wherein the portion is the public key.

15. The system of claim 13, wherein the firmware program further clears the upgrade flag.

16. The system of claim 13, further comprising:

a persistent storage, wherein the file is located in the persistent storage.

17. The system of claim 13, further comprising:

a network interface for connecting the system to a network, wherein the file is retrieved from the network.

18. The system of claim 13, the firmware program comprises a second portion further comprising:

a minimal boot portion;

a signature authentication portion; and

a write device portion.

19. The system of claim 13, wherein the portion of the firmware program further comprises:

a hardware initialization portion;

an operating system loader portion; and

a device lock-out portion.

20. The system of claim 18, wherein the portion of the firmware program further comprises:

the public key; and

a backup public key.

21. The system of claim 13, wherein the device is a flash memory.

22

19. A system comprising:

a file signed by a private key; and

a firmware program comprising a permanent portion and an upgradable portion, wherein the upgradable portion includes a first public key and a second public key, the firmware program further:

identifies a request to upgrade the firmware program;

experiences an interruption in execution during an upgrade of the first public key; and

upgrades the firmware program using the second public key once the interruption in execution is complete.

23

22. The system of claim 21, further comprising an upgrade flag with which the firmware program identifies the request to upgrade the firmware program.

24

23. The system of claim 22, wherein the interruption in execution is due to a power loss to the system.

25

24. The system of claim 22 further comprising a device for storing the firmware program wherein the device is locked such that the public keys are not writable after the firmware program is upgraded.

26

25. The system of claim 22, further comprising a device for storing the firmware program wherein the device is locked such that the public keys are not readable after the firmware program is upgraded.

26. An article comprising a medium storing instructions for enabling a processor-based system to:

identify a firmware upgrade request by a firmware program;

retrieve a file signed with a private key;

validate the file with a public key;

upgrade a portion of the firmware program by the firmware program; and

lock a device storing the firmware program such that the public key is not readable.

27. The article of claim 26, further storing instructions that enable the processor-based system to:

validate the public key; and

retrieve a second public key from the firmware program if the public key is not valid.

28. The article of claim 27, further storing instructions that enable the processor-based system to:

determine that the file is not authentic; and

lock the device.

29. An article comprising a medium storing instructions for enabling a processor-based system to:

identify an upgrade request for a firmware program of a system;

upgrade a first public key of the firmware program;

receive an interruption of power to the system;

use a second public key to subsequently upgrade the firmware program.

~~30~~. The article of claim 29, further storing instructions that enable the processor-based system to:

retrieve a file signed by a private key from the system; and

authenticate the file with the second public key.